

## THE FACTS: PHISHING

### *What is “phishing?”*

Email attack is the preferred method for many hackers -- a cybercriminal sends an email that attempts to fraudulently acquire the recipient's personal information or deliver malware. A phishing email might include an attachment or a link or request personal information.



The email may appear to be legitimate communication from your bank, phone company, a store you frequent, or a friend or coworker, and may include links to convincing fraudulent sites that often mimic popular online venues. A phishing email calls for an action, such as clicking on an embedded link, opening an attachment, or providing personal information.

Phishing scams work. Verizon's 2019 Data Breach Investigations Report showed that nearly a third of all data breaches online, and more than three-quarters of cyber-espionage attacks, involved phishing. And it's getting worse as perpetrators get better and phishing kits that make it easy for cyber criminals to send fraudulent emails and spoof trusted sites or brands become more available.

Additionally, on some sites that hackers love – social media and banking websites – emails are used as usernames. A hacker who knows his target's email address would then know their likely username for some accounts and could then try to crack the target's passwords on those accounts.

### *What are “spearphishing” and “whaling?”*

The higher up you are in an organization, the more likely you are to be a target for “spearphishing” -- specialized attacks against specific targets or small groups of targets to collect information or gain access to systems. In a spearphishing campaign, hackers have done their homework and learned names of the target's subordinates, associates, friends and perhaps even clubs the target belongs to or schools the target's children attend. Spearphishing emails typically appear to be from or about those close relations. “Whaling” defines attempts to specifically target high-value or senior personnel.

### *What are some ways to identify phishing emails?*

**Poor spelling and grammar.** Cyber criminals normally do not have the staff of copy editors professional companies or organizations have, so phishing attempts often contain spelling and grammar mistakes.

**Threats.** Have you ever received a threat that your account would be closed if you didn't respond to an email message? Cybercriminals often use threats that your security has been compromised.

**ABOUT US:** U.S. Army Cyber Command integrates and conducts full-spectrum cyberspace operations, electronic warfare, and information operations, ensuring freedom of action for friendly forces in and through the cyber domain and the information environment, while denying the same to our adversaries.

As of 21 February 2020

**Spoofing popular websites or companies.** Scam artists use graphics that appear to be connected to legitimate websites, but take you to scam sites or legitimate-looking pop-up windows. Cybercriminals also use web addresses that resemble the names of well-known companies but are slightly altered.

### ***What can I do to help avoid becoming a victim of phishing?***

**Beware of links in email.** Rest your mouse on the link (but don't click!) to see if the address matches the link typed in the message. Look at the example at left. The real address, shown in the small box, doesn't look anything like the link text or the company's web address.



**Call before you click.** Suppose you have an email that seems to be from your organization's human resources department telling you to complete an attached form to "update your personnel file." The attachment could be an executable malware file, or it could be a legitimate personnel update. Fight the natural instinct to trust an official-looking communication. Assume it's malware until proven otherwise.

**When in doubt, throw it out.** If it looks suspicious, even if you know the source, it's best to delete it or, if appropriate, mark it as junk email.

**Consider using specialized email accounts.** Use one account for work, one for friends and one for online purchases. If you create a unique email address just for online payments, for example, it will be harder for a hacker to gain access to your information and account.

**Take advantage of free security checkups.** For a list of free security checks for your computer, visit <http://www.staysafeonline.org/stay-safe-online/free-security-check-ups/>.

**If you are a victim of phishing, report it.** Report phishing attempts to the appropriate experts within your organization, such as network administrators and security officers. If you believe your financial accounts may be compromised, contact your financial institutions immediately. Additionally, consider reporting the attack to your local police department, the [Federal Trade Commission](#), the [Anti-Phishing Working Group](#) (APWG), and/or the FBI's [Internet Crime Complaint Center](#).

### ***What about phishing phone calls?***

Email isn't the only way criminals launch phishing attempts. They might also try to scam you by phone, claiming to represent a trusted firm. Once they gain your trust, they may ask you for user names or passwords or direct you to a website to install software that allows them to access your computer. Be wary of unsolicited calls and report them to your security manager and/or other appropriate authority.



**Follow ARCYBER on**  
(click the images to visit our pages)



**ABOUT US:** U.S. Army Cyber Command integrates and conducts full-spectrum cyberspace operations, electronic warfare, and information operations, ensuring freedom of action for friendly forces in and through the cyber domain and the information environment, while denying the same to our adversaries.

As of 21 February 2020